

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

Rec'd PCT/PTO 16 JUN 2005

10/539018

REC'D 01 MAR 2004

WIPO

PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 13 JAN. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

BEST AVAILABLE COPY

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

6 bis, rue de Saint Pétersbourg

5800 Paris Cedex 08

téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

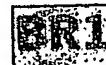
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle

N° 11354*02

REQUÊTE EN DÉLIVRANCE

page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W - 010301

REMISE DES PIÈCES DATE 18 DEC 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0216084 DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 18 DEC. 2002		NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE CABINET BONNET-THIRION 12, avenue de la Grande Armée 75017 PARIS	
Vos références pour ce dossier (facultatif) BIF114554/FR			
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
<input checked="" type="checkbox"/> Demande de brevet		<input checked="" type="checkbox"/>	
<input type="checkbox"/> Demande de certificat d'utilité		<input type="checkbox"/>	
<input type="checkbox"/> Demande divisionnaire		<input type="checkbox"/>	
<i>Demande de brevet initiale</i>		N°	Date
<i>ou demande de certificat d'utilité initiale</i>		N°	Date
<input type="checkbox"/> Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/>	Date
		N°	Date
TITRE DE L'INVENTION (200 caractères ou espaces maximum) Dispositif optimisé de communication de données numériques dans une carte à microcircuit.			
DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale Prénoms Forme juridique N° SIREN Code APE-NAF		OBERTHUR CARD SYSTEMS SA Société anonyme _____ _____ 102, Boulevard Malesherbes	
Domicile ou siège	Rue		
	Code postal et ville	75017 PARIS	
	Pays	FRANCE	
Nationalité	FRANCAISE		
N° de téléphone (facultatif)	N° de télécopie (facultatif)		
Adresse électronique (facultatif)			
		<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»	

BEST AVAILABLE COPY

Remplir impérativement la 2^{ème} page

Réservé à l'INPI

REMAISE DES PIÈCES

DATE **18 DEC 2002**

LIEU **75 INPI PARIS**

N° D'ENREGISTREMENT

0216084

NATIONAL ATTRIBUÉ PAR L'INPI

CB 5-0 W, 710502

6 MANDATAIRE <i>(s'il y a lieu)</i> Nom Prénom Cabinet ou Société N° de pouvoir permanent et/ou de lien contractuel Adresse Rue Code postal et ville Pays N° de téléphone <i>(facultatif)</i> N° de télécopie <i>(facultatif)</i> Adresse électronique <i>(facultatif)</i>		BIF 114554/FR CABINET BONNET-THIRION 12 Avenue de la Grande Armée 75017 PARIS FRANCE 01 53 81 17 00
7 INVENTEUR (S) Les demandeurs et les inventeurs sont les mêmes personnes		Les inventeurs sont nécessairement des personnes physiques <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)
8 RAPPORT DE RECHERCHE Établissement immédiat ou établissement différé		Uniquement pour une demande de brevet (y compris division et transformation) <input checked="" type="checkbox"/> Établissement immédiat <input type="checkbox"/> Établissement différé
Paiement échelonné de la redevance <i>(en deux versements)</i>		Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt <input type="checkbox"/> Oui <input type="checkbox"/> Non
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention <i>(joindre un acte de non-imposition)</i> <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention <i>(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)</i> AG
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS Le support électronique de données est joint La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		<input type="checkbox"/> Cochez la case si la description contient une liste de séquences <input type="checkbox"/>
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		
11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) Bruno QUANEN N°92.1206 CABINET BONNET-THIRION		VISA DE LA PRÉFECTURE OU DE L'INPI M. ROCHET

La présente invention concerne une carte à microcircuit.

Plus précisément, l'invention vise une carte à microcircuit adaptée :

- d'une part à traiter un flux relativement important de données numériques échangées avec un dispositif extérieur à la carte ; et

5 - d'autre part à mettre en œuvre des procédures de sécurisation, par exemple des fonctions de vérification de l'intégrité des données numériques échangées avec le dispositif extérieur ou des fonctions cryptographiques d'authentification d'un utilisateur de la carte.

10 L'invention pourra ainsi être utilisée pour la décompression d'un flux de données numériques cryptées.

15 Selon une architecture connue d'une telle carte, les données numériques reçues depuis un port d'entrée-sortie de la carte à microcircuit sont lues par un microprocesseur et traitées au fil de leur réception. Le microprocesseur effectue les contrôles de sécurité précités au fur et à mesure qu'il reçoit les données numériques.

 Un problème majeur de cette architecture est que le flux de données numériques pouvant être échangées par la carte est limité par la fréquence du microprocesseur (généralement de l'ordre de 4 MHz pour les cartes à microcircuit connues de l'état de la technique).

20 Dans d'autres domaines de l'électronique, pour palier les limites associées à la fréquence d'un microprocesseur, le transfert de données à haut débit est souvent réalisé par des composants dédiés appelés DMA (Direct Memory Access). Ces composants DMA sont programmés par un microprocesseur pour effectuer un transfert prédéterminé, par exemple entre un
25 port d'entrée-sortie et une mémoire, le transfert en tant que tel n'étant pas réalisé par le microprocesseur.

 Malheureusement, ces composants DMA sont dédiés au transfert de données et ne permettent pas d'effectuer de traitement sur les données au cours de leur transfert. Ils ne sont donc pas, a priori, adaptés pour le transfert de

données sensibles nécessitant des opérations de sécurisation, comme c'est le cas pour les cartes à microcircuit précitées.

5 L'invention vise, en surmontant cette apparente incompatibilité, à permettre un transfert d'un flux important ou rapide de données sécurisées dans une carte à microcircuit tout en maintenant un niveau de sécurité important, ce grâce à une association originale d'un processeur et d'un DMA.

Elle propose à cet effet une carte à microcircuit comportant :

- des moyens d'entrée-sortie de données numériques ;
- des moyens de traitement de ces données ; et
- 10 - des moyens de contrôle de flux.

La carte à microcircuit est caractérisée en ce que les moyens de traitement comportent :

- des moyens de transfert de ces données numériques entre les moyens d'entrée-sortie et une zone de mémorisation ; et
- 15 - des moyens de communication, avec les moyens de contrôle de flux, de données de sécurisation obtenues à partir des données numériques, les moyens de contrôle de flux étant adaptés à contrôler le transfert des données numériques par les moyens de transfert en prenant en compte ces données de sécurisation.

20 Ainsi, les données reçues depuis le port de communication sont transférées par les moyens de transfert vers une zone de mémorisation, le flux de ce transfert n'étant pas limité par la vitesse des moyens de contrôle de flux.

Par ailleurs, au cours de ce transfert, des données de sécurisation obtenues à partir des données numériques sont communiquées par les moyens
25 de traitement aux moyens de contrôle de flux, le flux de ces données de sécurisation reçues par les moyens de contrôle de flux étant limité et de toute façon bien inférieur au flux de données numériques reçues par la carte.

Les moyens de contrôle de flux, constitués par exemple par un processeur, sont alors à même d'effectuer, en utilisant ces données de
30 sécurisation, les opérations nécessaires de contrôle des moyens de transfert pour garantir le respect des contraintes de sécurité.

L'invention permet ainsi d'augmenter le flux de données numériques traitées par la carte à microcircuit, tout en maintenant le niveau de sécurité d'une carte traditionnelle.

5 Dans une première variante de réalisation de la carte à microcircuit selon l'invention, les données de sécurisation précitées sont constituées, au moins en partie, par une partie des données numériques transférées par la carte.

10 Dans un mode préféré de cette première variante de réalisation, les données de sécurisation comportent des données d'authentification d'une partie des données numériques reçues par la carte, les moyens de contrôle de flux étant adaptés à vérifier la validité des données numériques à partir de ces données d'authentification, et à contrôler le transfert en fonction du résultat de cette vérification.

15 De façon connue, lorsque la carte reçoit des données numériques transmises par un dispositif extérieur, si les moyens de contrôle de flux déterminent que les données d'authentification ne sont pas valides, cela signifie que les données numériques n'ont pas été envoyées par un émetteur autorisé.

Dans ce cas, les moyens de contrôle de flux peuvent prendre une mesure prédéterminée, telle que bloquer l'utilisation de la carte ou envoyer un message d'erreur.

20 Dans un mode préféré de réalisation, afin de garantir une utilisation sécurisée de la carte, les moyens de contrôle de flux commandent l'arrêt du transfert des données numériques par les moyens de transfert lorsque les données d'authentification ne sont pas valides.

25 La carte peut ainsi recevoir un flux important de données, une partie seulement de ces données étant communiquée aux moyens de contrôle de flux pour garantir la sécurité exigée.

Dans une deuxième variante de réalisation, les moyens de traitement sont adaptés à insérer dans les données de sécurisation un résultat de traitement calculé à partir des données numériques.

30 Le résultat de traitement peut par exemple être le résultat d'une étape de vérification des données d'authentification précitées par des moyens de calcul compris dans les moyens de traitement, par exemple des moyens cryptographiques de la carte à microcircuit. Ce résultat est ensuite pris en

compte par les moyens de contrôle de flux pour vérifier l'intégrité des données numériques et pour contrôler leur transfert par les moyens de transfert en conséquence.

5 Cette étape d'authentification peut consister à vérifier une signature, par exemple en utilisant une clef cryptographique et une fonction de hachage selon un algorithme du type MD4, MD5 ou SHA-1.

10 Dans cette variante, ce sont les moyens de contrôle de flux qui effectuent les étapes de vérification des données d'authentification. Ils peuvent ensuite prendre une mesure prédéterminée telle qu'arrêter le transfert des données numériques ou bloquer l'utilisation de la carte, en cas d'utilisation frauduleuse de celle-ci.

Dans un mode de réalisation préféré, les moyens de contrôle de flux effectuent le contrôle du transfert des données numériques en modifiant au moins un paramètre de fonctionnement des moyens de transfert.

15 Par exemple, ce paramètre de fonctionnement est une adresse de mémorisation des données numériques dans la zone de mémorisation.

20 Ainsi, lorsque le taux d'occupation d'une première plage de la zone de mémorisation est supérieur à un seuil prédéterminé, les moyens de contrôle de flux peuvent paramétrer les moyens de transfert pour que les données numériques reçues par les moyens de transfert soient mémorisées à cette adresse.

25 Le paramètre précité peut également être un paramètre permettant de sélectionner le protocole de communication entre les moyens d'entrée-sortie et la zone de mémorisation. Ce protocole de communication peut par exemple être adapté aux transferts de données sécurisées.

Selon différentes variantes de réalisation de la carte à microcircuit selon l'invention, les moyens de traitement comportent une unité de compression des données, une unité de décompression des données, une unité de cryptage des données ou une unité de décryptage des données.

30 Dans une autre variante de réalisation, les moyens de contrôle de flux sont en outre adaptés à obtenir des données préliminaires directement à partir des moyens d'entrée-sortie, les données préliminaires étant prises en compte

par l'unité de contrôle de flux pour autoriser ou refuser le transfert des données numériques par les moyens de transfert.

Dans un mode particulier de cette variante de réalisation, ces données préliminaires comportent des données d'authentification.

5 Ce mode de réalisation permet d'obtenir un niveau de sécurité supplémentaire, par exemple par le contrôle d'un code d'authentification, préalablement au transfert des données numériques proprement dites. Contrairement aux données de sécurité, ce code d'authentification n'est
10 demander plus de temps calcul, et donc mettre en œuvre un algorithme d'authentification complexe et permettant d'obtenir un niveau de sécurité renforcé.

Dans un autre mode de réalisation préféré, ces données préliminaires comportent une adresse de mémorisation des données numériques qui seront
15 transférées par les moyens de transfert. Dans ce mode de réalisation préféré, ces données préliminaires peuvent en outre comporter des données d'authentification de cette adresse de mémorisation, ceci afin de garantir que l'adresse de mémorisation n'a pas été fournie par un utilisateur non autorisé.

Selon un mode de réalisation particulièrement avantageux, la carte à
20 microcircuit comporte en outre des moyens de régulation adaptés à modifier une fréquence d'horloge appliquée aux moyens de traitement en fonction desdites données de sécurisation.

Cette caractéristique permet ainsi de limiter la consommation électrique de la carte à microcircuit lorsque le transfert de données numériques par les
25 moyens de transfert doit être interrompu.

L'invention sera mieux comprise et d'autres avantages apparaîtront plus clairement à la lumière de la description qui va suivre d'une carte à microcircuit conforme à son principe, donnée uniquement à titre d'exemple et faite en
référence aux dessins annexés dans lesquels :

- 30
- la figure 1 est un schéma bloc d'une carte à microcircuit conforme à la technique antérieure ;
 - la figure 2 est un schéma bloc analogue à la figure 1 illustrant un mode de réalisation possible d'une carte à microcircuit conforme à l'invention ; et

- la figure 3 est un exemple de données de sécurisation conformément à l'invention.

5 La carte à microcircuit 10 conforme à l'art antérieur représentée sur la figure 1 comporte principalement un processeur CPU associé de façon classique à un certain nombre de mémoires (du type RAM, ROM, EEPROM), des moyens de traitement 12 et des moyens d'entrée-sortie 14 reliés par exemple, à un terminal.

10 Les moyens de traitement 12 comportent une unité de calcul 13 adaptée à réaliser le traitement proprement dit des données numériques, à savoir par exemple des opérations de compression, de décompression, de cryptage ou de décryptage de ces données.

15 Dans un mode de réalisation préféré, les moyens d'entrée-sortie 14 permettant à la carte à microcircuit 10 de communiquer avec un terminal ou une entité électronique extérieure, comprennent essentiellement une unité d'émission réception asynchrone de type UART.

Les moyens d'entrée-sortie 14 peuvent aussi être adaptés à mettre en œuvre des protocoles de communication standardisés et connus de l'homme du métier, à savoir par exemple, les protocoles connus sous les références "T=0", "T=1" (ISO 7816), USB, FireWire ou I2C.

20 Selon l'art antérieur, lorsque la carte à microcircuit 10 reçoit via l'UART des données numériques qui doivent être soumises à un traitement par l'unité de calcul 13 des moyens de traitement 12, l'UART transmet un message d'interruption au processeur CPU. Le processeur CPU vient alors lire un registre de l'UART et copier les données dans la mémoire RAM.

25 Le processeur CPU initialise alors les moyens de traitement 12 puis va lire les données à traiter dans la mémoire RAM et les copie dans un registre 16 des moyens de traitement 12.

30 Afin d'être communiqué au terminal extérieur, le résultat calculé par les moyens de traitement 12 est ensuite lu par le processeur CPU dans le registre 16 et copié dans le registre UART par le processeur CPU.

Un tel mode de fonctionnement n'est pas favorable au traitement de données numériques à haut débit par la carte à microcircuit 10. En effet, l'opération intermédiaire réalisée par le processeur CPU de copie des données

numériques dans la zone de mémorisation RAM avant traitement par les moyens de traitement 12 est tout particulièrement pénalisante.

Or, on souhaite augmenter la puissance de traitement d'une telle carte à microcircuit pour traiter des flux importants et continus de données en temps réel.

A titre d'exemple, on souhaite pouvoir procéder au déchiffrement en temps réel de données numériques représentatives d'un son. De telles données sont compressées selon la norme MP3 et transmises à une vitesse de 128 kbits/s. La carte à microcircuit chargée du déchiffrement en temps réel nécessite donc de pouvoir recevoir et traiter des informations à haut débit.

Une carte à microcircuit conforme à l'invention et permettant de résoudre le problème précédent va maintenant être décrite en référence à la figure 2.

Conformément à la présente invention, les moyens de traitement 12 comportent des moyens de transfert DMA des données numériques entre le port de communication 14 et une zone de mémorisation 18.

Dans l'exemple de la figure 2 décrit ici, la zone de mémorisation 18 est une mémoire vive RAM.

Dans d'autres modes de réalisation, la zone de mémorisation 18 peut être choisie parmi différents types de mémoires réinscriptibles, à savoir par exemple, une mémoire Flash, une mémoire de type EEPROM ou un disque dur.

Dans une autre variante de réalisation, la zone de mémorisation 18 est un port de l'unité de calcul 13 des moyens de traitement 12.

Dans le mode de réalisation préféré décrit ici, ces moyens de transfert DMA comportent un composant électronique dédié connu de l'homme du métier appelé DMA (Direct Memory Access).

De façon connue, de tels composants se programment par l'écriture de paramètres dans des registres de configuration.

A titre d'exemple non limitatif, de tels paramètres comportent l'adresse d'un port des moyens d'entrée-sortie 14, l'adresse d'une plage de la zone de mémorisation 18 dans laquelle les données numériques doivent être mémorisées, et des paramètres représentatifs d'un critère d'arrêt du transfert.

Quoiqu'il en soit, la carte à microcircuit selon l'invention comporte en outre des moyens de contrôle de flux 26 adaptés à contrôler le transfert des données numériques par les moyens de transfert DMA.

5 En particulier, lorsque les données numériques doivent être transférées vers une zone de mémorisation 18 de type EEPROM, les moyens de contrôle de flux 26 sont adaptés à contrôler un générateur de tension ou tout autre moyen permettant d'appliquer une tension électrique suffisante à la mémoire EEPROM pour que celle ci soit accessible en écriture.

10 Dans le mode de réalisation décrit en référence à la figure 2, les moyens de contrôle de flux 26 sont constitués par un processeur CPU, lequel est classiquement associé à ces différentes mémoires (RAM, ROM, EEPROM) comme dans le cas de la figure 1.

Le paramétrage des moyens de transfert DMA par les moyens de contrôle de flux 26 est représenté schématiquement par les signaux 20 à la figure 2.

15 Conformément à la présente invention, les moyens de traitement 12 comportent également des moyens de communication 22 entre son unité de calcul 13 et les moyens de contrôle de flux 26.

20 Ces moyens de communication 22 permettent l'échange de données de sécurisation entre les moyens de traitement 12 et les moyens de contrôle de flux 26, ces données de sécurisation étant obtenues à partir des données numériques DATA transférées par les moyens de transfert DMA.

25 Chronologiquement, une fois les moyens de transfert DMA programmés par les moyens de contrôle de flux 26 au moyen des signaux 20, les moyens de transfert DMA réalisent le transfert des données numériques entre les moyens d'entrée-sortie 14 et la zone de mémorisation 18. L'unité de calcul 13 des moyens de traitement 12 obtient ensuite les données de sécurisation DATA_CTRL à partir des données numériques DATA mémorisées dans la zone de mémorisation 18 et les communique aux moyens de contrôle de flux 26 par les moyens de communication 22.

30 Un exemple de données de sécurisation DATA_CTRL, dans un mode préféré de réalisation, est donné à la figure 3.

Les données de sécurisation DATA_CTRL comportent une partie P1 des données numériques et des données d'authentification AUTH calculées à partir des données numériques de la partie P1.

5 Dans une première variante de réalisation, les données d'authentification AUTH forment une signature de P1. Typiquement, il s'agit des données P1 auxquelles on a appliqué, une fonction de Hachage connue tel que MD4, MD5 ou SHA-1, puis un algorithme de cryptage. Pour cela, on peut utiliser un algorithme de cryptage à clef symétrique tel que l'algorithme DES (Data Encryption Standard) ou un algorithme à clef asymétrique tel que l'algorithme
10 RSA (du nom de ses inventeurs Rivest, Shamir et Adelman).

Dans cette variante, sur réception de ces données de sécurisation DATA_CTRL, les moyens de contrôle de flux 26 décryptent tout d'abord la signature AUTH avec la clef de décryptage et obtiennent un premier résultat HASH1. Les moyens de contrôle de flux 26 appliquent ensuite la fonction de
15 hachage à la partie P1 et obtiennent un deuxième résultat HASH2.

Les moyens de contrôle de flux 26 comparent ensuite le premier résultat HASH1 et deuxième résultat HASH2.

Dans un mode de réalisation préféré de cette première variante, lorsque ces résultats HASH1 et HASH2 diffèrent, les moyens de contrôle de flux 26 commandent l'arrêt du transfert des données numériques par l'envoi d'un signal d'arrêt.
20

Dans le mode de réalisation préféré, les moyens de traitement 12 insèrent dans les données de sécurisation DATA_CTRL un résultat de traitement des données numériques DATA par l'unité de calcul 13.

25 Ce résultat de traitement est par exemple l'adresse à laquelle une partie des données numériques DATA a été mémorisée par les moyens de transfert DMA dans la zone de mémorisation 18, les moyens de contrôle de flux 26 étant alors adaptés à lire les données de cette partie, à en vérifier la validité, et à contrôler le transfert des données numériques DATA par les moyens de transfert
30 DMA en fonction du résultat de cette vérification.

Dans un mode de réalisation dans lequel les moyens de traitement 12 comportent des moyens cryptographiques 13, ce résultat de traitement est le

résultat, obtenu par l'unité cryptographique 13, d'une étape d'authentification des données numériques DATA.

5 En variante, le résultat de traitement est le résultat, obtenu par les moyens cryptographiques 13, d'une étape de vérification d'une signature des données numériques DATA.

Cette étape de vérification peut par exemple être le décryptage des données AUTH, ce décryptage étant réalisé en utilisant un algorithme RSA pour obtenir un résultat similaire au premier résultat HASH1.

10 Dans un mode de réalisation préféré, les moyens de contrôle de flux 26 sont en outre adaptés à obtenir des données préliminaires directement à partir des moyens d'entrée-sortie 14, par le chemin de données 24 représenté à la figure 2.

15 En variante, les données préliminaires sont obtenues par les moyens de contrôle de flux 26 à partir d'un deuxième port d'entrée-sortie, par exemple en utilisant le protocole connu sous la référence "T=0" (ISO 7816), les moyens d'entrée-sortie 14 étant réservés au transfert des données numériques DATA par les moyens de transfert DMA.

20 Le chemin de données 24 peut également être un chemin de données bidirectionnel utilisé par les moyens de contrôle de flux 26 pour communiquer des informations à un dispositif extérieur à la carte à microcircuit. Ces informations peuvent par exemple être constituées par un message d'erreur émis par les moyens de contrôle de flux 26 lorsque ceux-ci détectent, à partir des informations de sécurisation, la présence de données numériques erronées.

25 Ces informations peuvent également être constituées par un flux de données sortant de la carte à microcircuit, ce flux de données étant le résultat du traitement, par les moyens de traitement 12, des données numériques DATA reçues par la carte.

30 Ces données préliminaires comportent par exemple des données d'authentification PASSWD, ces données préliminaires étant quoi qu'il en soit prises en compte pour contrôler le transfert des données numériques par les moyens de transfert DMA.

Ainsi, par exemple si les données d'authentification PASSWD ne sont pas conformes à une règle de contrôle prédéterminée, cette règle pouvant être

mémorisée dans la mémoire ROM, les moyens de contrôle de flux 26 ne programment pas les moyens de transfert DMA pour réaliser le transfert de données numériques entre les moyens d'entrée-sortie 14 et la zone de mémorisation 18.

5 Préférentiellement, les données préliminaires comportent une adresse de mémorisation des données numériques.

Dans une variante de réalisation, la carte à microcircuit comporte des moyens de régulation PLL adaptés à modifier une fréquence d'horloge appliquée aux moyens de traitement 12 en fonction des données de contrôle DATA_CTRL.

10 Ces moyens de régulation PLL peuvent par exemple être constitués par un composant de type PLL (Phase Lock Looping en anglais) connu de l'homme du métier et permettant de dériver des signaux de différentes fréquences d'horloge, à partir d'un signal d'une horloge externe non représentée.

15 Dans le mode préféré de réalisation ces moyens de régulation PLL sont commandés par les moyens de contrôle de flux 26 afin d'ajuster la consommation électrique des moyens de traitement 12 en fonction du flux de données numériques DATA.

20 Selon le mode de réalisation choisi, les moyens de transfert DMA peuvent être unidirectionnels ou bidirectionnels. L'invention s'applique en particulier pour contrôler le transfert de données numériques cryptées DATA à partir de la zone de mémorisation 18 vers les moyens d'entrée-sortie 14.

REVENDICATIONS

1. Carte à microcircuit comportant :

- des moyens d'entrée-sortie (14) de données numériques (DATA) ;
- des moyens de traitement (12) de ces données ; et
- des moyens de contrôle de flux (26),

la carte à microcircuit étant caractérisée en ce que les moyens de traitement (12) comportent :

- des moyens de transfert (DMA) desdites données numériques (DATA) entre les moyens d'entrée-sortie (14) et une zone de mémorisation (18) ; et

- des moyens de communication (20), avec les moyens de contrôle de flux (26), de données de sécurisation (DATA_CTRL) obtenues à partir desdites données numériques (DATA),

les moyens de contrôle de flux (26) étant adaptés à contrôler le transfert des données numériques (DATA) par les moyens de transfert (DMA) en prenant en compte lesdites données de sécurisation (DATA_CTRL).

2. Carte à microcircuit selon la revendication 1, caractérisée en ce que lesdites données de sécurisation (DATA_CTRL) sont constituées au moins en partie par une partie desdites données numériques (DATA).

3. Carte à microcircuit selon la revendication 2, caractérisée en ce que lesdites données de sécurisation (DATA_CTRL) comportent des données d'authentification (AUTH) d'une partie (P1) des données numériques reçues par la carte, les moyens de contrôle de flux (26) étant adaptés à vérifier la validité desdites données numériques (DATA) à partir de ces données d'authentification (AUTH) et à contrôler ledit transfert en fonction du résultat de cette vérification.

4. Carte à microcircuit selon l'une quelconque des revendications 1 à 3, caractérisée en ce que lesdits moyens de traitement (12) sont adaptés à insérer dans lesdites données de sécurisation (DATA_CTRL), un résultat de traitement desdites données numériques (DATA).

5. Carte à microcircuit selon la revendication 4 caractérisée en ce que ledit résultat de traitement est le résultat d'une étape d'authentification desdites données numériques.

5

6. Carte à microcircuit selon l'une quelconque des revendications 1 à 5, caractérisée en ce que les moyens de contrôle de flux sont adaptés à modifier au moins un paramètre de fonctionnement desdits moyens de transfert (DMA).

10

7. Carte à microcircuit selon la revendication 6 caractérisée en ce que ledit paramètre est choisi parmi une adresse de ladite zone de mémorisation (18) et un paramètre de sélection d'un protocole de communication entre les moyens d'entrée-sortie (14) et la zone de mémorisation (18).

15

8. Carte à microcircuit selon l'une quelconque des revendications 1 à 7, caractérisée en ce que lesdits moyens de traitement (12) comportent une unité (13) de compression de données, une unité de décompression de données, une unité de cryptage de données, ou une unité de décryptage de données.

20

9. Carte à microcircuit selon l'une quelconque des revendications 1 à 8, caractérisée en ce que lesdits moyens de contrôle de flux (26) sont adaptés à arrêter le transfert des données numériques (DATA) par lesdits moyens de transfert (DMA) lorsqu'ils détectent, à partir desdites données de sécurisation (DATA_CTRL), la présence de données d'authentification invalides parmi lesdites données numériques (DATA).

25

10. Carte à microcircuit selon l'une quelconque des revendications 1 à 9 caractérisée en ce que les moyens de contrôle de flux (26) sont en outre adaptés à obtenir des données préliminaires directement à partir des moyens d'entrée-sortie (14), les données préliminaires étant également prises en compte par les moyens de contrôle de flux (26) pour autoriser ou refuser le transfert des données numériques (DATA) par les moyens de transfert (DMA).

30

11. Carte à microcircuit selon la revendication 10, caractérisée en ce que ~~lesdites données préliminaires comportent des données d'authentification~~ (PASSWD).

5 13. Carte à microcircuit selon la revendication 11 ou 12, caractérisée en ce que lesdites données comportent une adresse de mémorisation desdites données numériques.

10 14. Carte à microcircuit selon l'une quelconque des revendications 1 à 13, caractérisée en ce qu'elle comporte en outre des moyens de régulation (PLL) adaptés à modifier une fréquence d'horloge appliquée aux moyens de traitement (12) en fonction desdites données de sécurisation (DATA_CTRL).

15 15. Carte à microcircuit selon l'une quelconque des revendications 1 à 14, caractérisée en ce que lesdits moyens de transfert (DMA) comportent un composant DMA.

11. Carte à microcircuit selon la revendication 10, caractérisée en ce que lesdites données préliminaires comportent des données d'authentification (PASSWD) .

5 12. Carte à microcircuit selon la revendication 10 ou 11, caractérisée en ce que lesdites données préliminaires comportent une adresse de mémorisation desdites données numériques.

10 13. Carte à microcircuit selon l'une quelconque des revendications 1 à 12, caractérisée en ce qu'elle comporte en outre des moyens de régulation (PLL) adaptés à modifier une fréquence d'horloge appliquée aux moyens de traitement (12) en fonction desdites données de sécurisation (DATA_CTRL).

15 14. Carte à microcircuit selon l'une quelconque des revendications 1 à 13, caractérisée en ce que lesdits moyens de transfert (DMA) comportent un composant DMA.

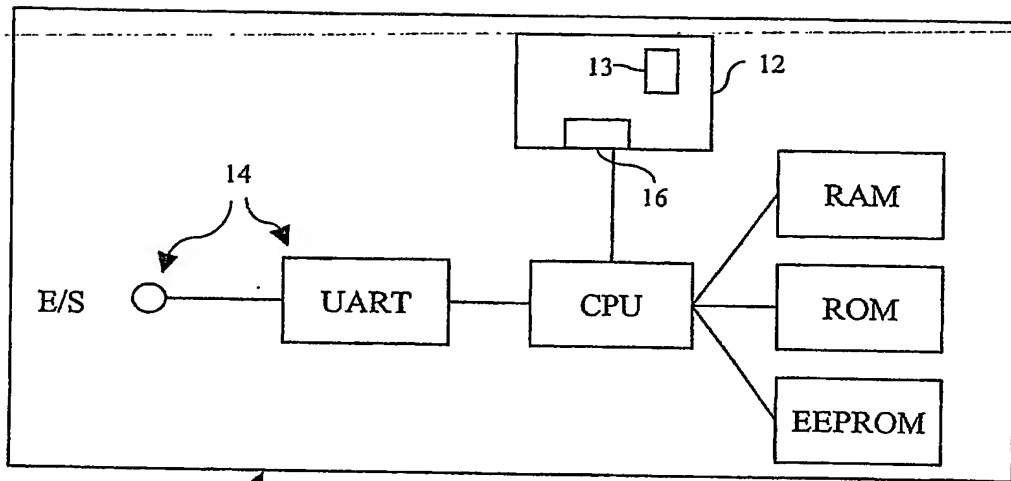


FIGURE 1

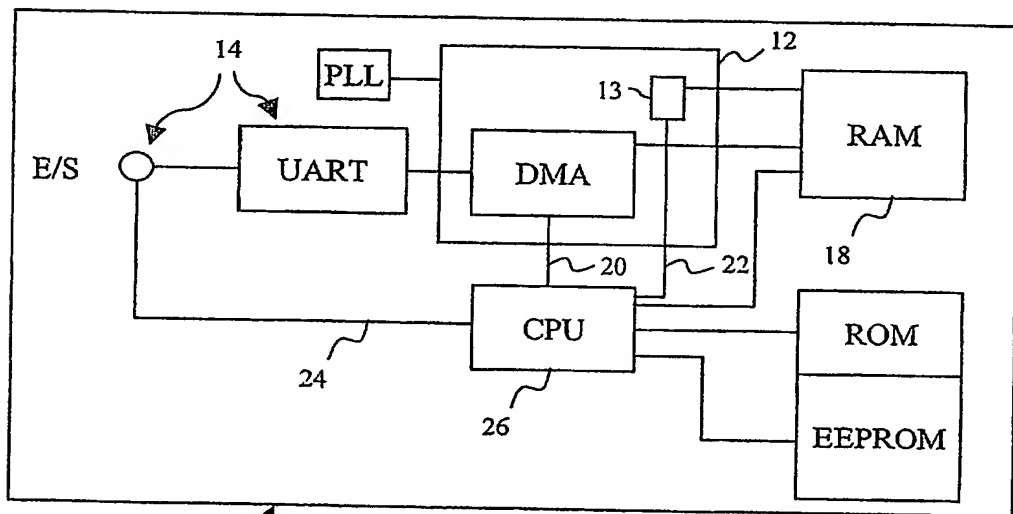


FIGURE 2

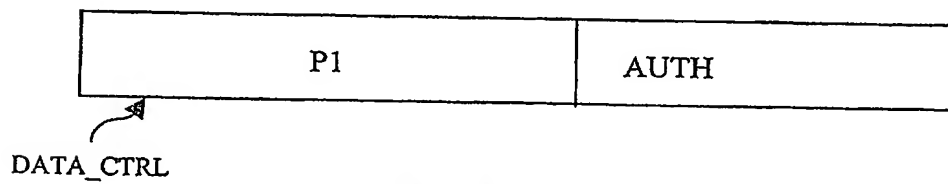


FIGURE 3

**BREVET D'INVENTION****CERTIFICAT D'UTILITÉ**

Code de la propriété intellectuelle - Livre VI

**DÉPARTEMENT DES BREVETS**

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° ... / ...

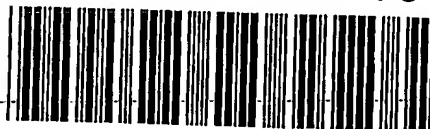
(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

08 113 W / 27C

Vos références pour ce dossier (facultatif)		BIF114554/FR
N° D'ENREGISTREMENT NATIONAL		
TITRE DE L'INVENTION (200 caractères ou espaces maximum)		
Dispositif optimisé de communication de données numériques dans une carte à microcircuit.		
LE(S) DEMANDEUR(S) :		
OBERTHUR CARD SYSTEMS SA		
DESIGNE(NT) EN TANT QU'INVENTEUR(S) :		
1	Nom	GOUESSANT
	Prénoms	Hervé
Adresse	Rue	25 impasse André Kommer,
	Code postal et ville	94410 Vitry-sur-Seine, France
Société d'appartenance (facultatif)		
2	Nom	JAYET
	Prénoms	Stéphane
Adresse	Rue	25 Allée des Noisetiers
	Code postal et ville	95250 Beauchamp, France
Société d'appartenance (facultatif)		
3	Nom	
	Prénoms	
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		
S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.		
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		
Le 28 janvier 2003 Bruno QUANTIN N°92.1206 CABINET BONNET-THIRION		

PCT Application
PCT/FR2003/003773



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.